On the face of the patent, please amend the related U.S. Application Data (Section 63) as follows:

Continuation in part of PCT/US96/06618 filed May 7, 1996, and a continuation-in-part of Ser. No. 637,531, Apr. 25, 1996, and a continuation-in-part of Ser. No. 534,005, Sep. 25, 1995, and a continuation-in-part of Ser. No. [598,083] 508,083, Jul. 27, 1995, and a continuation-in-part of Ser. No. 436,102, May 8, 1995, Pat. No. 5,748,783, and a continuation-in-part of Ser. No. 327,426, Oct. 21, 1994, Pat. No. 5,768,426, which is a continuation-in-part of Ser. No. 215,289, Mar. 17, 1994, abandoned, which is a continuation-in-part of Ser. No. 154,866 Nov. 18, 1993, abandoned. Application No. 08/637,531, filed April 25, 1996, is a continuation in part of Application No. 08/512,993, filed August 9, 1995 (abandoned).

In the Specification:

Column 1, lines 6-17, please amend the paragraph as follows:

This application is a continuation in part of the following copending applications: PCT/US96/06618 (May 7, 1996), Ser. No. 08/637,531 (filed Apr. 25, 1996) allowed, Ser. No. 08/534,005 (filed Sep. 25, 1995) allowed, Ser. No. [08/598,083] 08/508,083 (filed Jul. 27, 1995) pending, Ser. No. 08/436,102 (filed May 8, 1995) now U.S. Pat. No. 5,778,783, and Ser. No. 08/327,426 (filed Oct. 21, 1994) now U.S. Pat. No. 5,768,426. This later application is a continuation-in-part of Ser. No. 08/215,289 (filed Mar. 17, 1994), now abandoned, which is a continuation-in-part of Ser. No. 08/154,866 (filed Nov. 18, 1993), also abandoned. Application No. 08/637,531, filed April 25, 1996, claims priority to Application No. 08/512,993, filed August 9, 1995 (abandoned). Application No. 08/637,531, filed April 25, 1996, is a continuation in part of Application No. 08/512,993, filed August 9, 1995 (now abandoned). Priority is claimed to each of these prior applications.

Column 1, line 19, after the section entitled "Related Application Data" and before the section entitled "Background and Summary of the Invention", please insert the following paragraph:

REFERENCE TO COMPUTER PROGRAM LISTING

The file of this patent includes duplicate copies of a compact disc with a file entitled "Appendix B.txt", created on January 27, 2004, and having a size of 375,829 bytes (376,832 bytes on disc), which is hereby incorporated by reference.

Column 2, line 9, please amend the paragraph as follows:

FIG. 11 shows a process flow for detecting a standard noise code that can be used in the FIG. 10 embodiment.

Column 8, lines 16-30 , please amend the paragraph as follows:

Next we experiment visually with adding the composite embedded signal to the original digital image, through varying the X and Y parameters of equation 2. In formula, we visually iterate to both maximize X and to find the appropriate Y in the following:

$V_{dist;n,m} = V_{orig;n,m} + \cancel{[V_{compn,m}]}\ \underline{V_{comp;n,m}} * X * sqrt(4 + V_{orig;n,m}\ {}^\wedge Y)$ (3)

where dist refers to the candidate distributable image, i.e. we are visually iterating to find what X and Y will give us an acceptable image; orig refers to the pixel value of the original image; and comp refers to the pixel value of the composite image. The n's and m's still index rows and columns of the image and indicate that this operation is done on all 4000 by 4000 pixels. The symbol V is the DN of a given pixel and a given image.

Column 13, lines 31-42, please amend the paragraph as follows:

So, bearing in mind this additional item of signal coupling, the identification process now estimates the signal amplitude of each and every individual embedded code signal (as opposed to taking the cross-correlation result of step 12, FIG. 3). If our identification signal exists in the suspect picture, the amplitudes thus found will split into a polarity with positive amplitudes being assigned a `1` and negative amplitudes being assigned a [`1`]`0`. Our unique identification code manifests itself. If, on the other hand, no such identification code exists or it is someone else's code, then a random gaussian-like distribution of amplitudes is found with a random hash of values.

Column 16, lines 56-64, please amend the paragraph as follows:

In particular, a pointer 230 is cycled sequentially through the bit positions of the code word in register 216 to provide a control bit of "0" or "1" to a control input 232 of the adder/subtracter 212. If, for a particular input signal sample, the control bit is a "1", the scaled noise signal sample on line [32] 232 is added to the input signal sample. If the control bit is a "0", the scaled noise signal sample is subtracted from the input signal sample. The output 234 from the adder/subtracter 212 provides the black box's output signal.

At Column 25, lines 14-50, please amend the paragraph as follows:

The use of libraries of universal codes simply means that applicant's techniques are employed as described, except for the fact that only a limited set of the individual embedded code signals are generated and that any given encoded material will make use of some sub-set of this limited "universal set." An example is in order here. A photographic print paper manufacturer may wish to pre-expose every piece of 8 by 10 inch print paper which they sell with a unique identification code. They also wish to sell identification code recognition software to their large customers, service bureaus, stock agencies, and individual photographers, so that all these people can not only verify that their own material is correctly marked, but so that they can also determine if third party material which they are about to acquire has been identified by this

technology as being copyrighted. This latter information will help them verify copyright holders and avoid litigation, among many other benefits. In order to "economically" institute this plan, they realize that generating unique individual embedded codes for each and every piece of print paper would generate Terabytes of independent information, which would need storing and to which recognition software would need access. Instead, they decide to embed their print paper with 16 bit identification codes derived from a set of only 50 independent "universal" embedded code signals. The details of how this is done are in the next paragraph, but the point is that now their recognition software only needs to contain a limited set of embedded codes in their library of [10] codes, typically on the order of 1 Megabyte to 10 Megabytes of information for 50x16 individual embedded codes splayed out onto an 8.times.10 photographic print (allowing for digital compression). The reason for picking 50 instead of just 16 is one of a little more added security, where if it were the same 16 embedded codes for all photographic sheets, not only would the serial number capability be limited to 2 to the 16th power, but lesser and lesser sophisticated pirates could crack the codes and remove them using software tools.

Column 30, lines 42-63, please amend the paragraph as follows:

The above case deals only with a single bit plane of information, i.e., the noise signature signal is either there (1) or it isn't (0). For many applications, it would be nice to detect serial number information as well, which could then be used for more complex decisions, or for logging information on billing statements or whatnot. The same principles as the above would apply, but now there would be N independent noise signatures as depicted in FIG. 9 instead one single such signature. Typically, one such signature would be the master upon which the mere existence of a copyright marking is detected, and this would have generally higher power than the others, and then the other lower power "identification" noise signatures would be embedded into audio. Recognition circuits, once having found the existence of the primary noise signature, would then step through the other N noise signatures applying the same steps as described above. Where a beat signal is detected, this indicates the bit value of `1`, and where no beat signal is

detected, this indicates a bit value of `0`. It might be typical that N will equal 32, that way [232] $\underline{2^{32}}$ number of identification codes are available to any given industry employing this technology.

Column 35, lines 25-29, please amend the paragraph as follows:

Another alternative is to use variable bit length codes such as the ones used in text compression routines [(e.g. Huffinan)] <u>(e.g. Huffman)</u> whereby more frequently used symbols have shorter bit length codes and less frequently used symbols have longer bit lengths.

Column 35, lines 32-46, please amend the paragraph as follows:

Classically speaking, the detection of the N-bit identification word fits nicely into the old art of detecting known signals in noise. Noise in this last statement can be interpreted very broadly, even to the point where an image or audio track itself can be considered noise, relative to the need to detect the underlying signature signals. One of many references to this older art is the book Kassam, Saleem A., "Signal Detection in Non-Gaussian Noise," Springer-Verlag, 1988 (generally available at well stocked libraries, e.g. available at the U.S. Library of Congress by catalog number TK5102.5 .K357 1988<u>)</u>. To the best of this inventor's current understanding, none of the material in this book is directly applicable to the issue of discovering the polarity of applicant's embedded signals, but the broader principles are indeed applicable.

Column 35, line 61 through Column 36, line 20, please amend the paragraph as follows:

The continued and inevitable engineering improvement in the detection of embedded code signals will undoubtedly borrow heavily from this generic field of known signal detection. A common and well-known technique in this field is the so-called "matched filter," which is incidentally discussed early in section 2 of the Kassam book. Many basic texts on signal processing include discussions on this method of signal detection. This is also known in some fields as correlation detection. Furthermore, when the phase or location of a known signal is known a priori, such as is often the case in applications of this technology, then the matched filter

can often be reduced to a simple vector dot product between a suspect image and the embedded signal associated with an m'th bit plane in our N-bit identification word. This then represents yet another simple "detection algorithm" for taking a suspect image and producing a sequence of [Is and Os] 1s and 0s with the intention of determining if that series corresponds to a pre-embedded N-bit identification word. In words, and with reference to FIG. 3, we run through the process steps up through and including the subtracting of the original image from the suspect, but the next step is merely to step through all N random independent signals and perform a simple vector dot product between these signals and the difference signal, and if that dot product is negative, assign a `0` and if that dot product is positive, assign a `1.` Careful analysis of this "one of many" algorithms will show its similarity to the traditional matched filter.

Column 40, lines 46-56, please amend the paragraph as follows:

The concept of the "header" on a digital image or audio file is a well established practice in the art. The top of FIG. 16 has a simplified look at the concept of the header, wherein a data file begins with generally a comprehensive set of information about the file as a whole, often including information about who the author or copyright holder of the data is, if there is a copyright holder at all. This header 800 is then typically followed by the data itself 802, such as an audio stream, [a image] a digital image, a video stream, or compressed versions of any of these items. This is all exceedingly known and common in the industry.

Column 43, lines 12-34, please amend the paragraph as follows:

Digital Video And Internet Company XYZ has developed a delivery system of its product which relies on a non-symmetric universal coding which double checks incoming video to see if the individual frames of video itself, the visual data, contain XYZ's own relatively high security internal signature codes using the methods of this technology. This works well and fine for many delivery situations, including their Internet tollgate which does not pass any material unless both the header information is verified AND the in-frame universal codes are found. However, another piece of their commercial network performs mundane routine monitoring on Internet

channels to look for unauthorized transmission of their proprietary creative property. They control the encryption procedures used, thus it is no problem for them to unencrypt creative property, including headers, and perform straightforward checks. A pirate group that wants to traffic material on XYZ's network has determined how to modify the security features in XYZ's header information system, and they have furthermore discovered that by simply rotating imagery by 10 or [20 degree;] <u>20 degrees</u>, and transmitting it over XYZ's network, the network doesn't recognize the codes and therefore does not flag illicit uses of their material, and the receiver of the pirate's rotated material simply unrotates it.

Column 43, line 66, through Column 44, line 18, please amend the paragraph as follows:

The "ring" is the only full rotationally symmetric two dimensional object. The "disk" can be seen as a simple finite series of concentric and perfectly abutted rings having width along their radial axis. Thus, the "ring" needs to be the starting point from which a more robust universal code standard for images is found. The ring also will fit nicely into the issue of scale/magnification changes, where the radius of a ring is a single parameter to keep track of and account for. Another property of the ring is that even the case where differential scale changes are made to different spatial axes in an image, and the ring turns into an oval, many of the smooth and quasi-symmetric properties that any automated monitoring system will be looking for are generally maintained. Likewise, appreciable geometric distortion of any image will clearly distort rings but they can still maintain gross symmetric properties. Hopefully, more pedestrian methods such as simply "viewing" imagery will be able to detect attempted illicit piracy in these regards, especially when such [lengths. are] <u>lengths are</u> taken to by-pass the universal coding system.

Column 45, lines 9-38, please amend the paragraph as follows:

A procedure for, first, checking for the mere existence of these knot patterns and, second, for reading of the N-bit identification word, is as follows. A suspect image is first fourier transformed via the extremely common 2D FFT computer procedure. Assuming that we don't

know the exact scale of the knot patterns, i.e., we don't know the radius of an elemental ring of the knot pattern in the units of pixels, and that we don't know the exact rotational state of a knot pattern, [vie] we merely inspect (via basic automated pattern recognition methods) the resulting magnitude of the Fourier transform of the original image for telltale ripple patterns (concentric low amplitude sinusoidal rings on top of the spatial frequency profile of a source image). The periodicity of these rings, along with the spacing of the rings, will inform us that the universal knot patterns are or are not likely present, and their scale in pixels. Classical small signal detection methods can be applied to this problem just as they can to the other detection methodologies of this disclosure. Common spatial filtering can then be applied to the fourier transformed suspect image, where the spatial filter to be used would pass all spatial frequencies which are on the crests of the concentric circles and block all other spatial frequencies. The resulting filtered image would be fourier transformed out of the spatial frequency domain back into the image space domain, and almost by visual inspection the inversion or non-inversion of the luminous rings could be detected, along with identification of the MSB or LSB ring, and the (in this case 8) N-bit identification code word could be found. Clearly, a pattern recognition procedure could perform this decoding step as well.

Column 53, lines 34-48, please amend the paragraph as follows:

The simplest way to use the principles of this technology in an exact steganographic system is to utilize the previously discussed "designed" master noise scheme wherein the master snowy code is not allowed to contain zeros. Both a sender and a receiver of information would need access to BOTH the master snowy code signal AND the original unencoded original signal. The receiver of the encoded signal merely subtracts the original signal giving the difference signal and the techniques of simple polarity checking between the difference signal and the master snowy code signal, data sample to data sample, producing a the passed message a single bit at a time. Presumably data samples with values near the "rails" of the grey value range would be skipped (such as the values [0,1 254] 0, 1, 254 and 255 in 8-bit depth empirical data).

Column 80, lines 30-41, please amend the paragraph as follows:

The process works in reverse when receiving. A broadcast from the cell cite is received through the antenna 2026. RF section 2024 amplifies and translates the received signal to a different frequency for demodulation. Demodulator 2028 processes the amplitude and/or phase variations of the signal provided by the RF section to produce a digital data stream corresponding thereto. The data unformatter 2030 segregates the voice data from the associated synchronization/control data, and passes the voice data to the [DIA] D/A converter for conversion into analog form. The output from the D/A converter drives the speaker 2034, through which the subscriber hears the other party's voice.

At column 90, line 61, after the paragraph ending with "A lightbulb is one suitable logo." please insert the following paragraph:

Appendix B

Applicant is preparing a steganographic marking/decoding "plug-in" for use with Adobe Photoshop software. The latest version of this software, presented as commented source code, is included in the file of this patent on a compact disc in a file named Appendix B.txt, created on January 27, 2004, and having a size of 375,829 bytes (376,832 bytes on disc), which is incorporated by reference. The code was written for compilation with Microsoft's Visual C++ compiler, version 4.0, and can be understood by those skilled in the art.

Please add to the file of the patent the compact discs containing Appendix B.